Kaspersky Industrial Cybersecurity Conference 2023

Обновления KICS

Стрелков Андрей
Руководитель направления развития продуктов для промышленной безопасности

kaspersky

Содержание

Основные направления развития

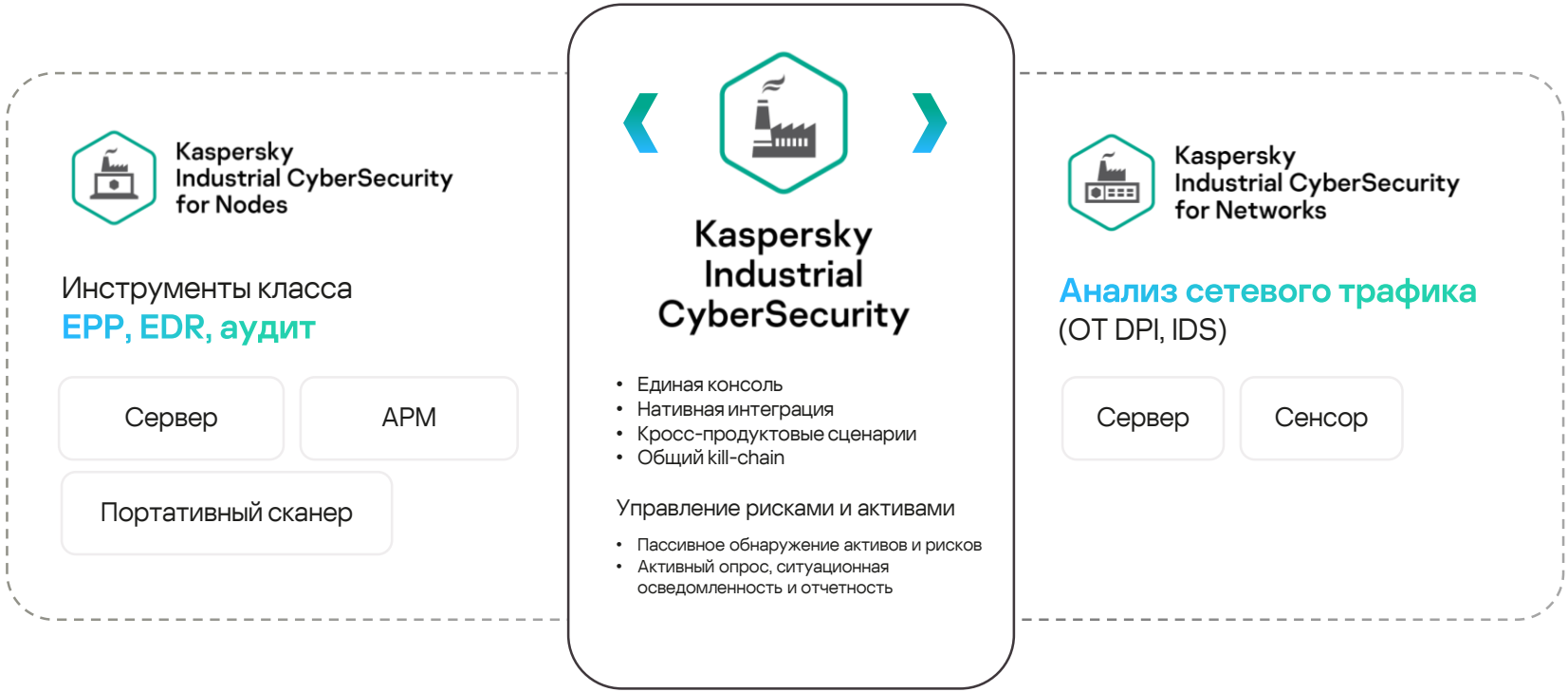
2023

OT XDR
Платформа для расширенного детектирования и реагирования на угрозы для промышленных сред

Аудит безопасности
Централизованная система для аудита безопасности узлов промышленной сети

NTA
Комплексный анализ сетевого трафика

Архитектура промышленной нативной OT XDR-платформы



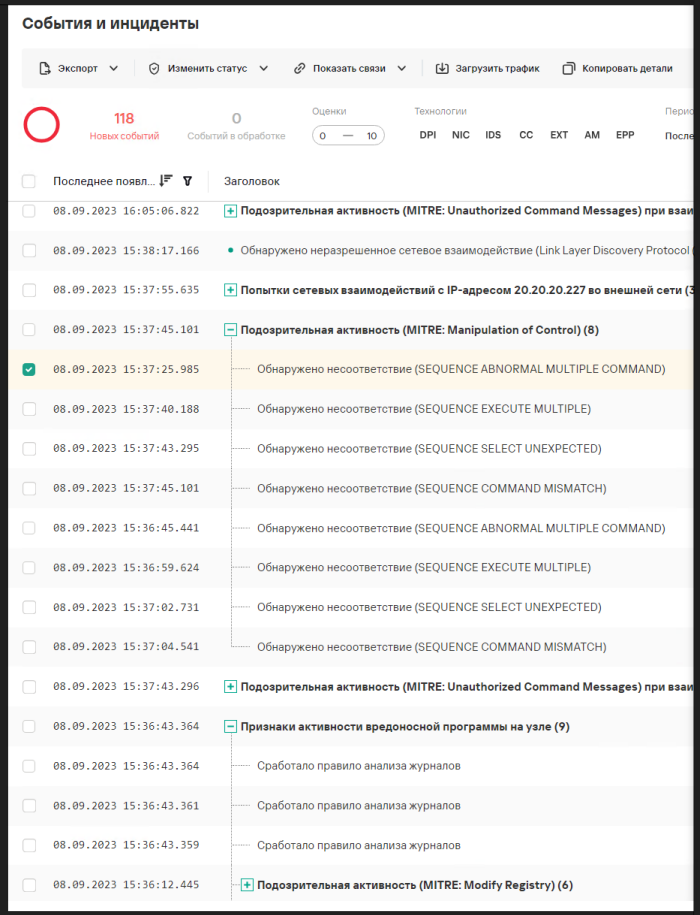
Нативная* система для расширенного детектирования и реагирования на угрозы

* Нативная – значит состоящая только из продуктов ЛК:
KICS for Nodes + KICS for Networks

Для ОТ сегмента
Подходит для изолированных промышленных сетей и для команд ИБ АСУ ТП

Только базовые решения
Сетевой и узловой сенсоры.

Управление на сервере KICS for Networks, не нужно дополнительное оборудование или лицензии



В KICS for Networks уже агрегируются и коррелируются все события от сенсоров на узлах и сети

Карточка сетевого детекта

- Детали актива
- Описание события
- Информация о приложении
- Список IoC

9.6 Обнаружено несоответствие (SEQUENCE ABNORMAL MULTIPLE COMMAND)

Изменить статус | Показать связи | Реагирование на угрозы | Создать разрешающее правило | Загрузить трафик

Возможные последствия:

- Отключение устройств.
- Изменение конфигураций устройств.
- Изменение параметров технологического процесса.

Меры по устранению угроз:

- Определить инициатора события по адресной информации (IP-адрес, MAC-адрес) и отключить от сети при несанкционированном подключении или несоответствии требуемым функциям.
- Проверить работу сетевого оборудования и средств защиты информации и при необходимости изменить параметры.
- Если событие зарегистрировано в результате замены оборудования и новое оборудование разрешено для использования, создайте разрешающее правило по технологии Контроль системных команд.

Приложение

Поставщик	Siemens AG, PTD EA
Название	RC-PCSW-CFE
Версия	2.22.13
Путь	C:\Program Files (x86)\Siemens Energy\SICAM\PAS PQS\CFE\Bin\CfeIEC104Slave.exe
Операционная система	Microsoft Windows 7
Адрес стороны взаимодействия	172.17.0.235:49432
Является сервером	Нет
Подпись	Недействительная
MD5	d1daf7170987525fe2aec0c4d7926c08
SHA256	b6900bd74df374e5f966bd727426d642e3feb1e21e8a098d0691308904dc41cc

Пользователь приложения

Имя	SICAM-PAS\PASRuntimeUser
Тип учетной записи	Не администратор
Тип входа	Прокси

Приложение

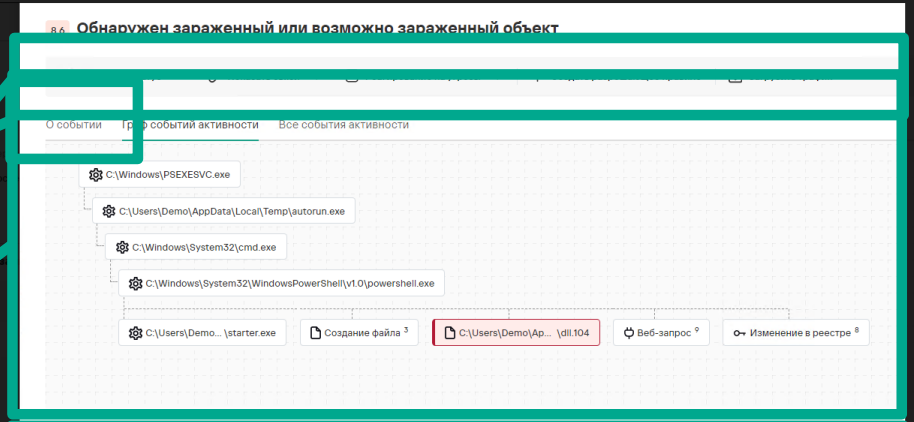
Поставщик	–
Название	–
Версия	–
Путь	C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\starter.exe
Операционная система	Microsoft Windows Server 2012 R2 Standard
Адрес стороны взаимодействия	172.17.0.235:49432
Является сервером	Нет
Подпись	Недействительная
MD5	c93c8d4ea47ee7d68f4830333e94e388
\256	edff1f8ab0bb74cb2957a02a978f2ff31a96cba78f6643701cb949bce4e36672

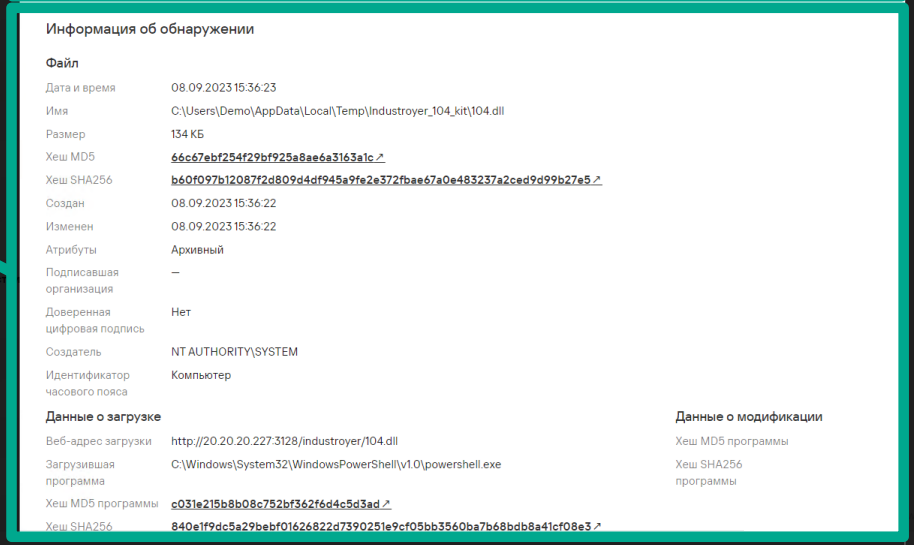
Пользователь приложения

Имя	RDC\RDC$
Тип учетной записи	Не администратор
Тип входа	Не определен

Карточка EDR-детекта:

- Детали актива
- Описание события
- Цепочка атаки на узле
- Список IoC
- Реагирование





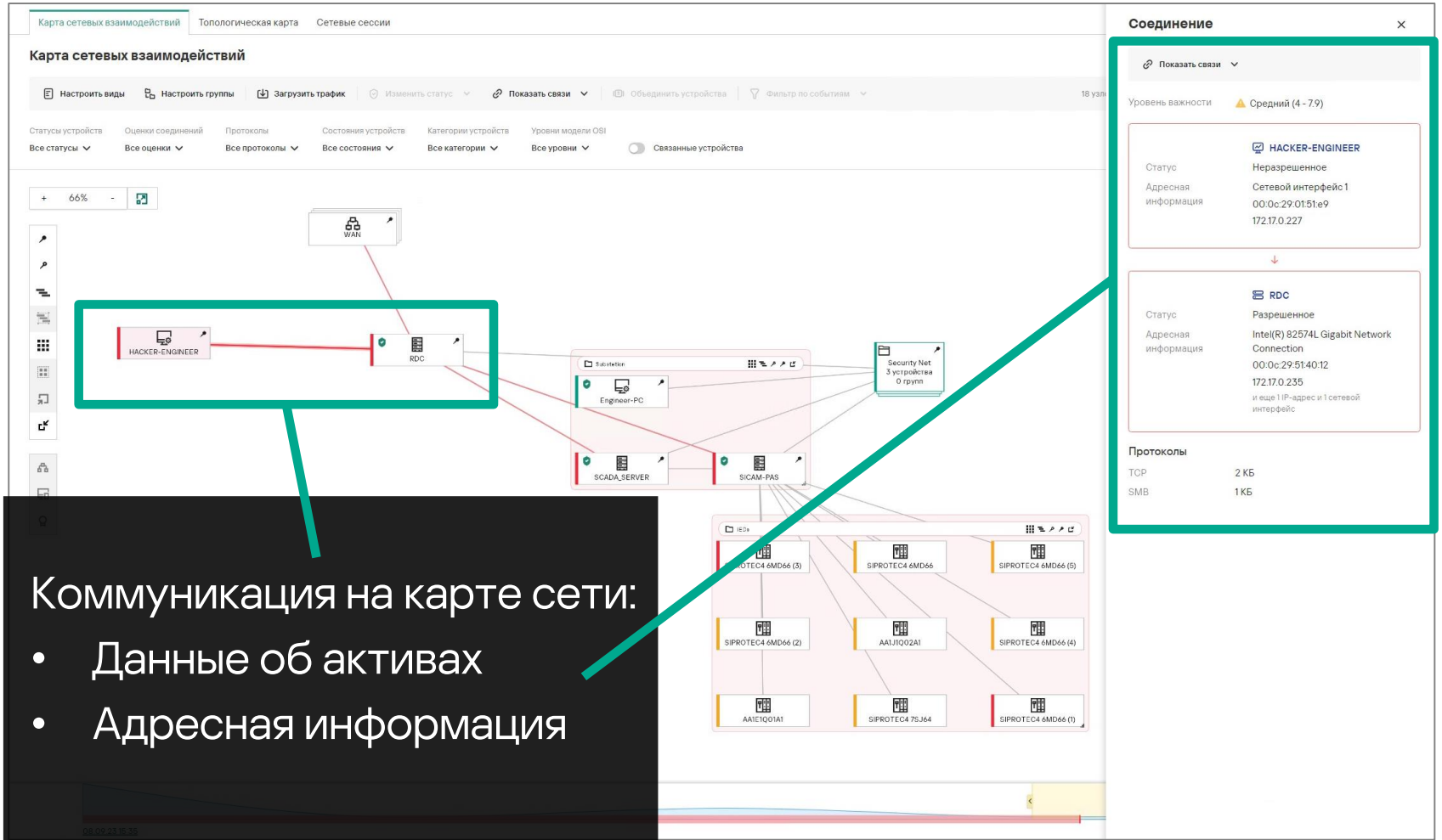
Анализ трафика внутри периметра инфраструктуры объекта

Разбирает как промышленные, так и корпоративные протоколы

Отображение сессий
Список всех сетевых сессий с детальной информацией для расследования инцидентов

Сохранение трафика и загрузка PCAP
Сохранение «сырого» трафика для последующего анализа

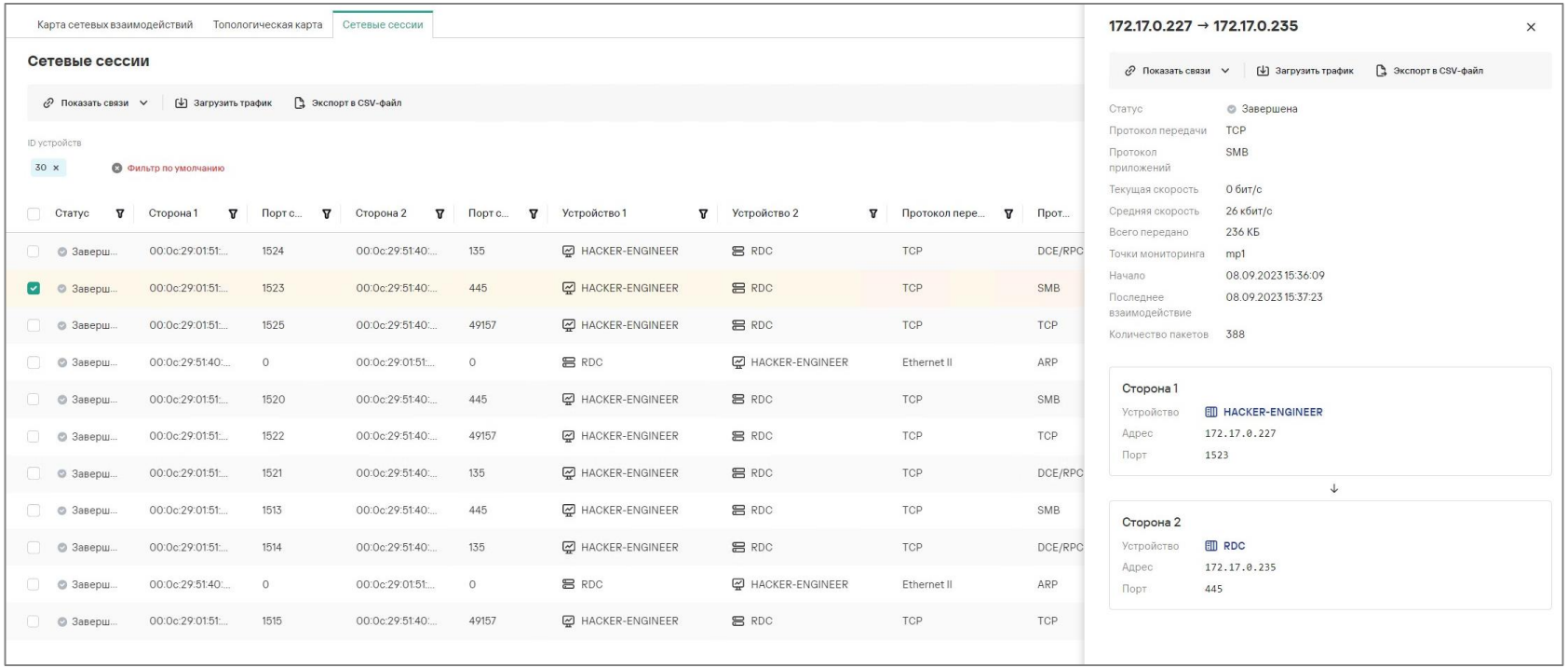
Новый модуль для поиска статистических аномалий и атак в сетевом трафике (брутфорс, спуфинг)

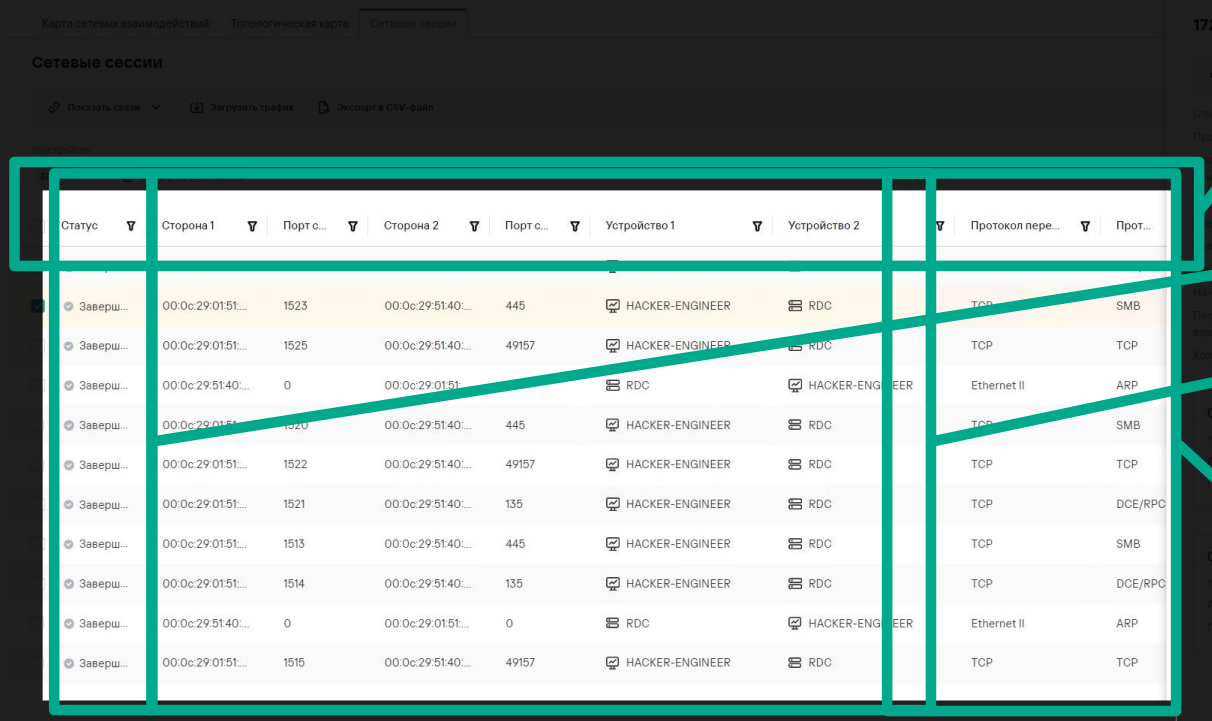


Коммуникация на карте сети:

- Данные об активах
- Адресная информация

Новая вкладка – Список сетевых сессий



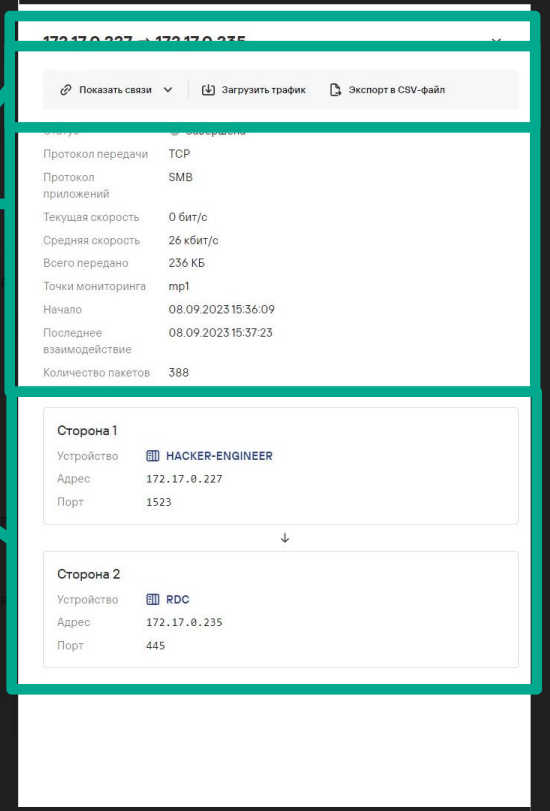


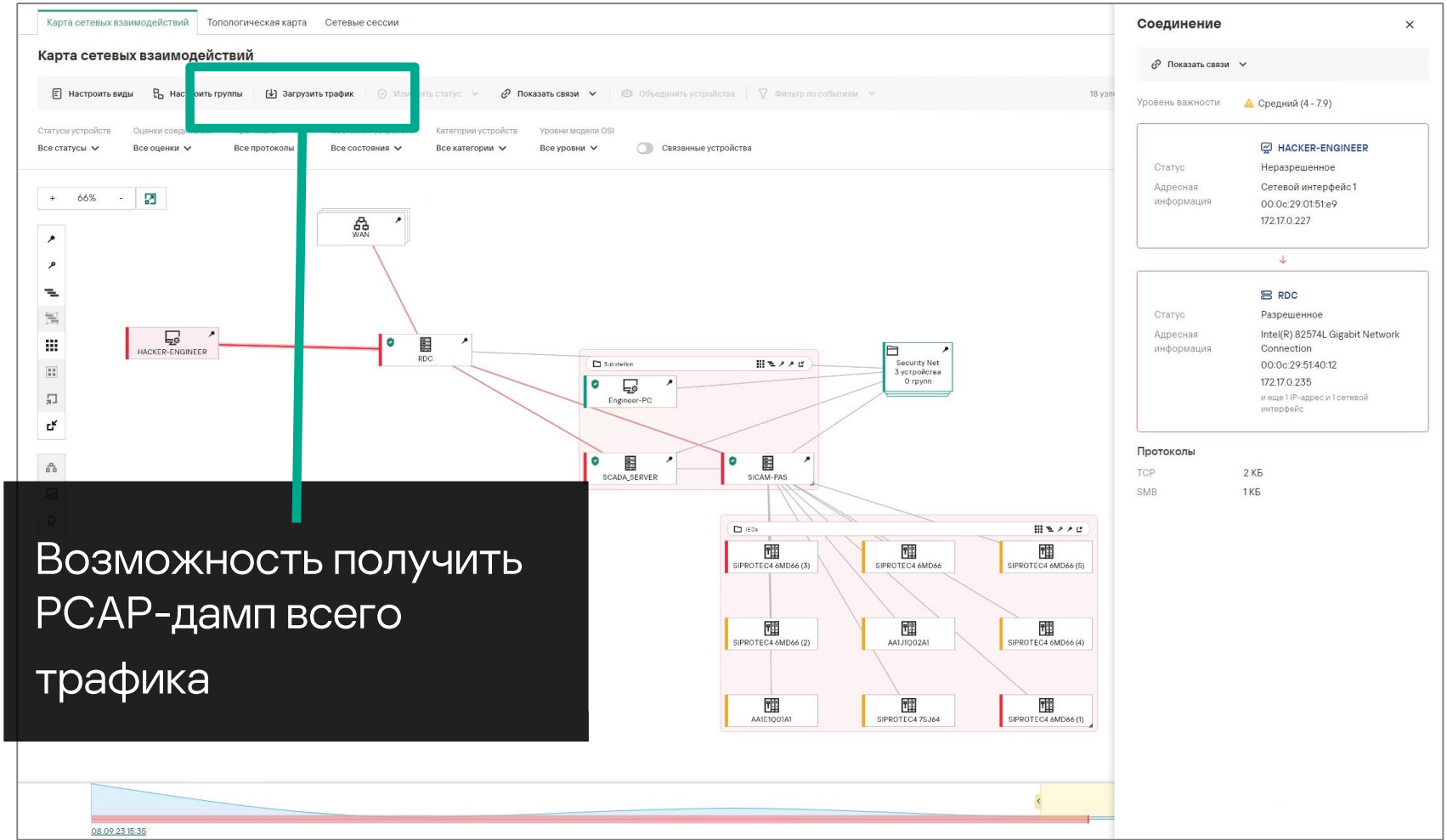
Список сессий:

- Полная информация о всех сессиях в рамках коммуникации
- Статус сессии
- Данные об активах
- Адресная информация, порты
- Протоколы
- Объем переданных данных/текущая скорость сессии
- Время начала и окончания

Карточка сессии:

- Детальная информация о выбранной сессии
- Переходы на карточки активов
- Возможность загрузить PCAP-дамп выбранной сессии

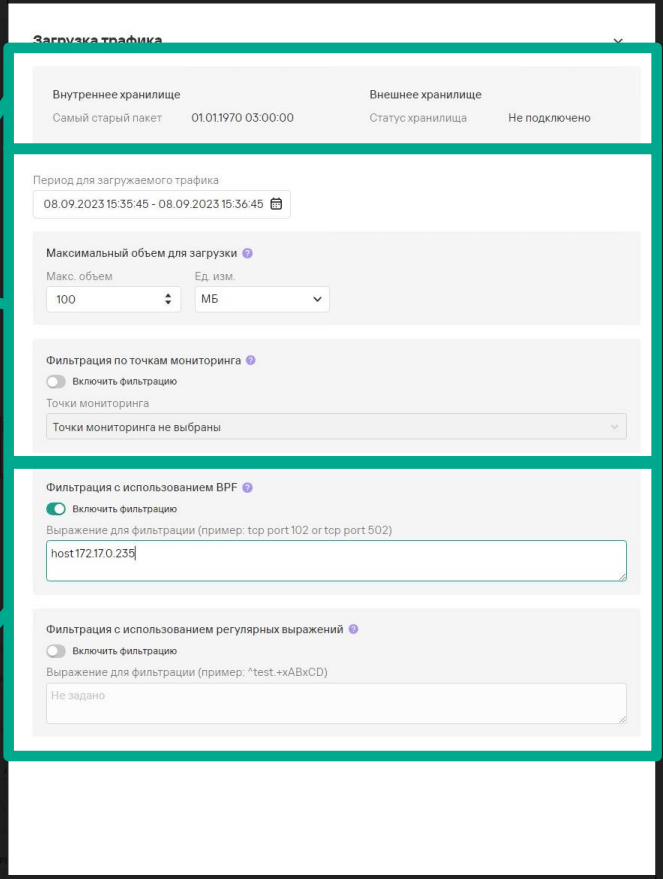




Возможность получить PCAP-дамп всего трафика

Загрузка трафика:

- Авто-сбор со всех Сенсоров и точек мониторинга за заданный период
- Внутреннее «встроенное» хранилище
- Внешнее подключаемое хранилище для больших объемов данных или длительного периода хранения
- Фильтрация пакетов с помощью BPF как для сохранения, так и для загрузки трафика



Ключевые преимущества

Аудит безопасности для узлов на Windows, Linux и сетевого оборудования

Открытый язык описаний Open Vulnerability and Assessment Language (OVAL)

Полнофункциональный редактор для проверок и параметров безопасности

Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT

Задачи для одного узла или групповые, запускаемые вручную или по расписанию

Поддержка сторонних и пользовательских баз OVAL

Отчёты, результаты аудита и история проверок доступны в одном месте

Защищённое хранилище секретов для безагентского аудита

Опрос устройств для аудита

Безагентский

Linux рабочие станции и серверы, сетевое оборудование

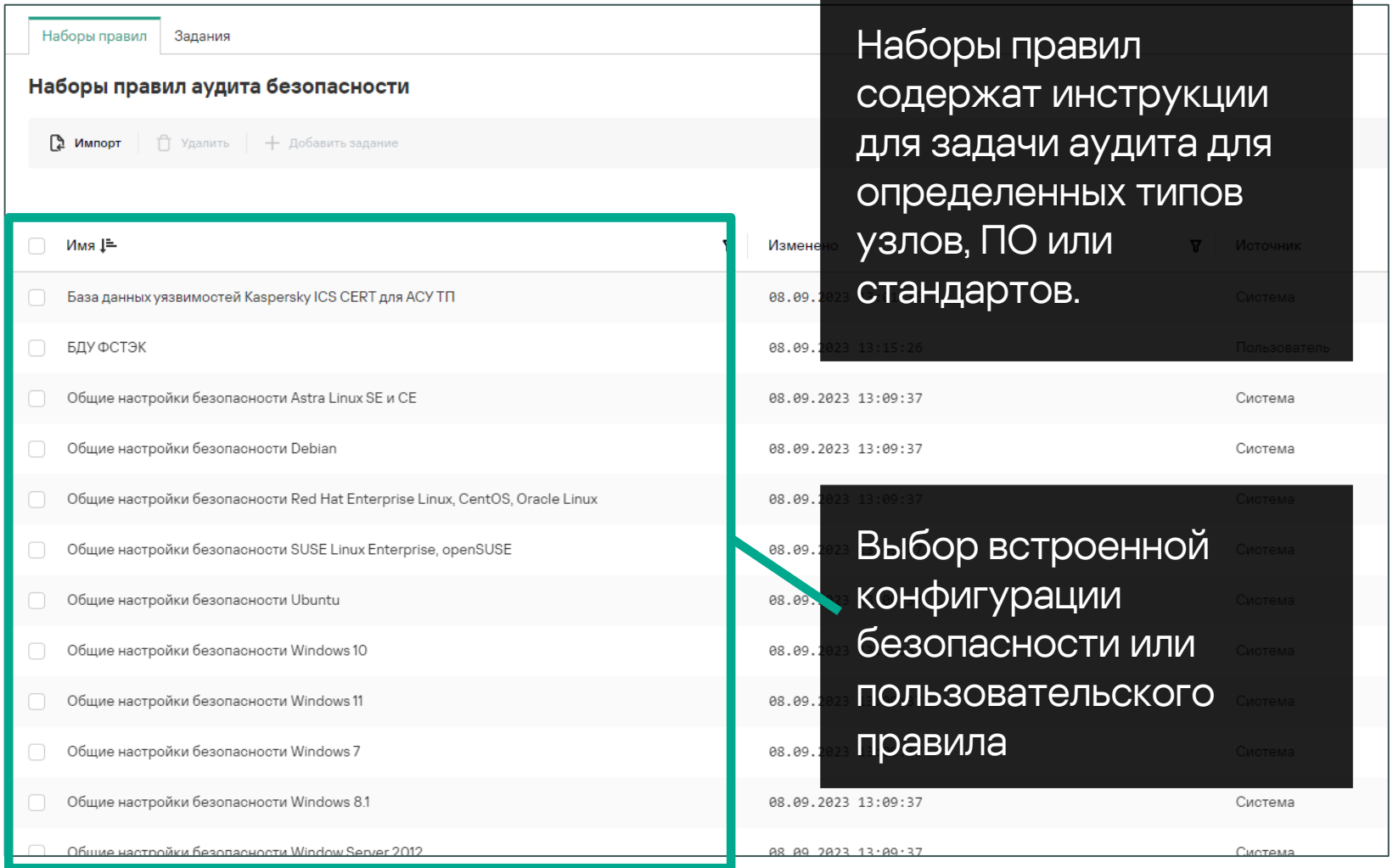
Требуется учетная запись

Через Агент

Windows рабочие станции и серверы

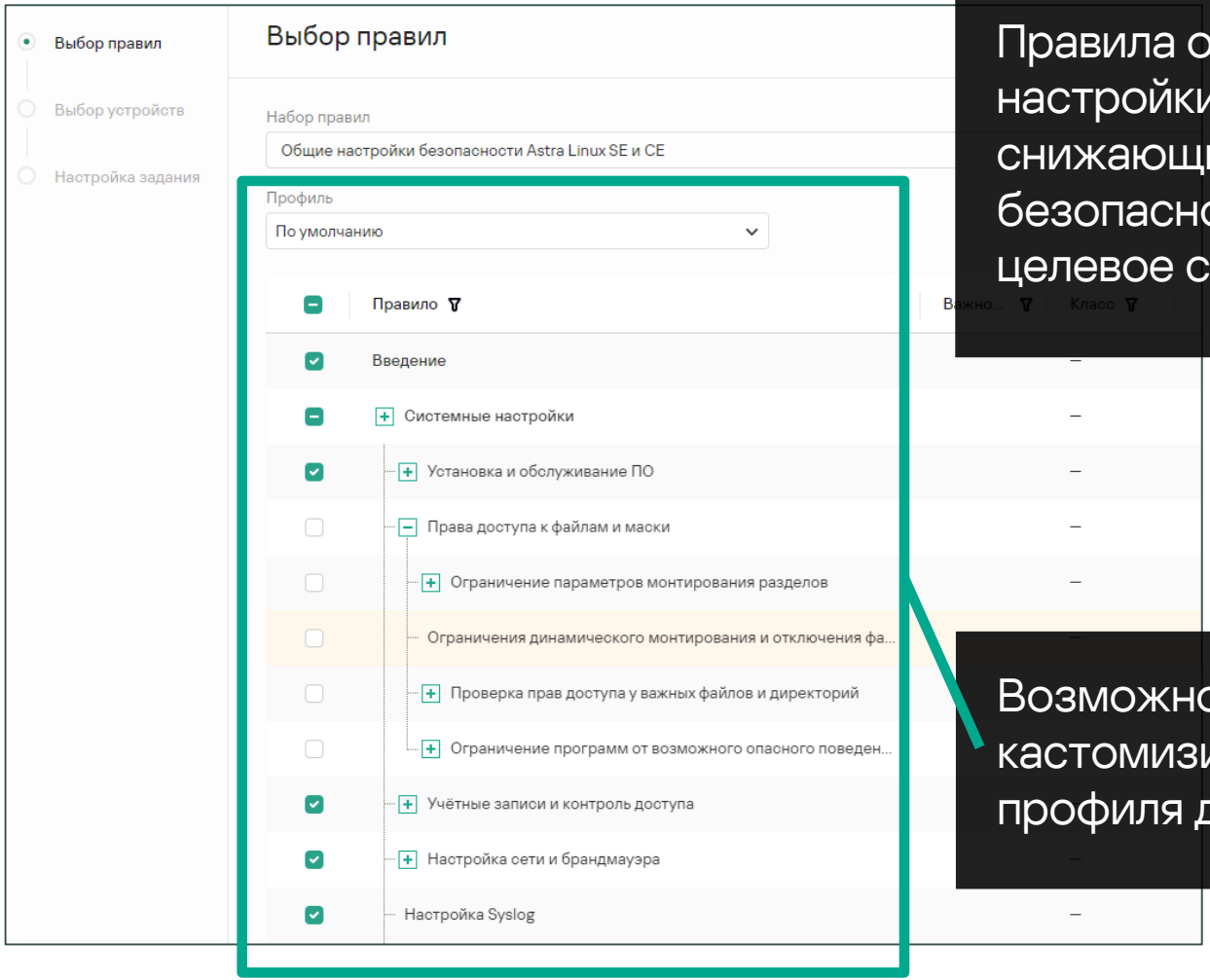
(Linux в 2024)

Не требуется учетная запись



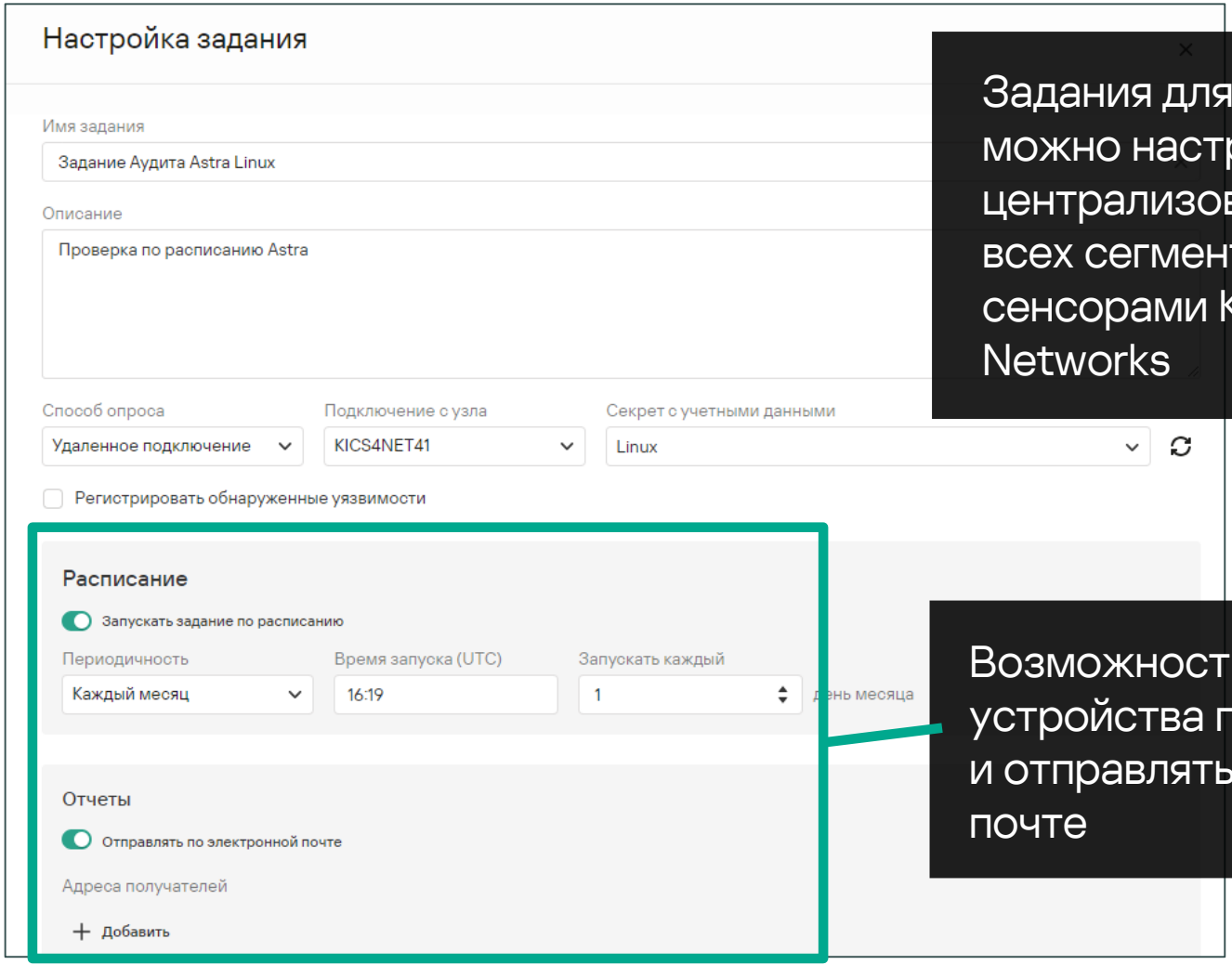
Наборы правил содержат инструкции для задачи аудита для определенных типов узлов, ПО или стандартов.

Выбор встроенной конфигурации безопасности или пользовательского правила



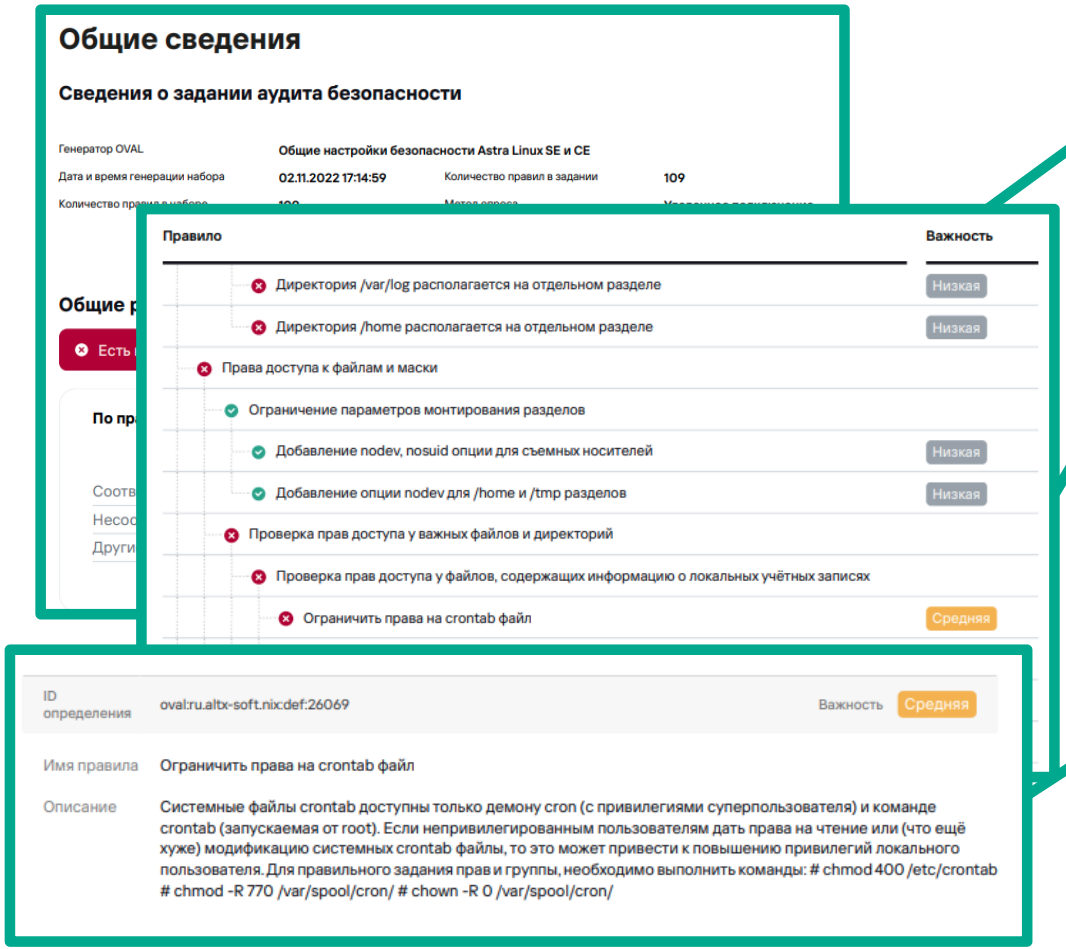
Правила описывают настройки системы, снижающие ее безопасность, и их целевое состояние.

Возможность задания кастомизированного профиля для аудита



Задания для аудита можно настраивать централизованно для всех сегментов с сенсорами KICS for Networks

Возможность опрашивать устройства по расписанию и отправлять отчеты по почте



После выполнения формируется pdf-отчет

Отчет содержит сводку и результаты проверок

По всем несоответствиям инструкция по устранению

Минорные обновления

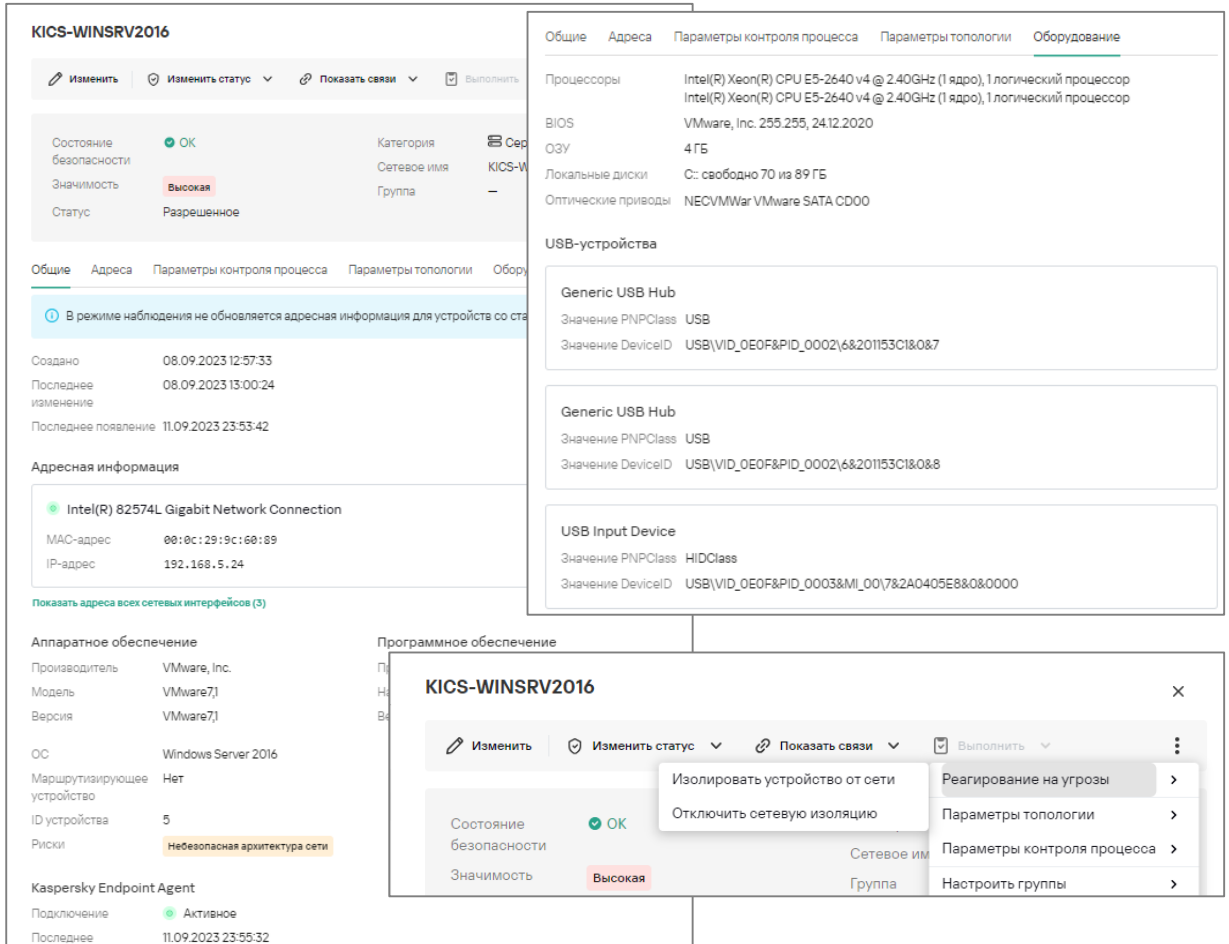
2023

Гранулярные настройки обучения KICS for Networks

Улучшения UI KICS for Networks

Улучшения KICS for Nodes

Обновления UI

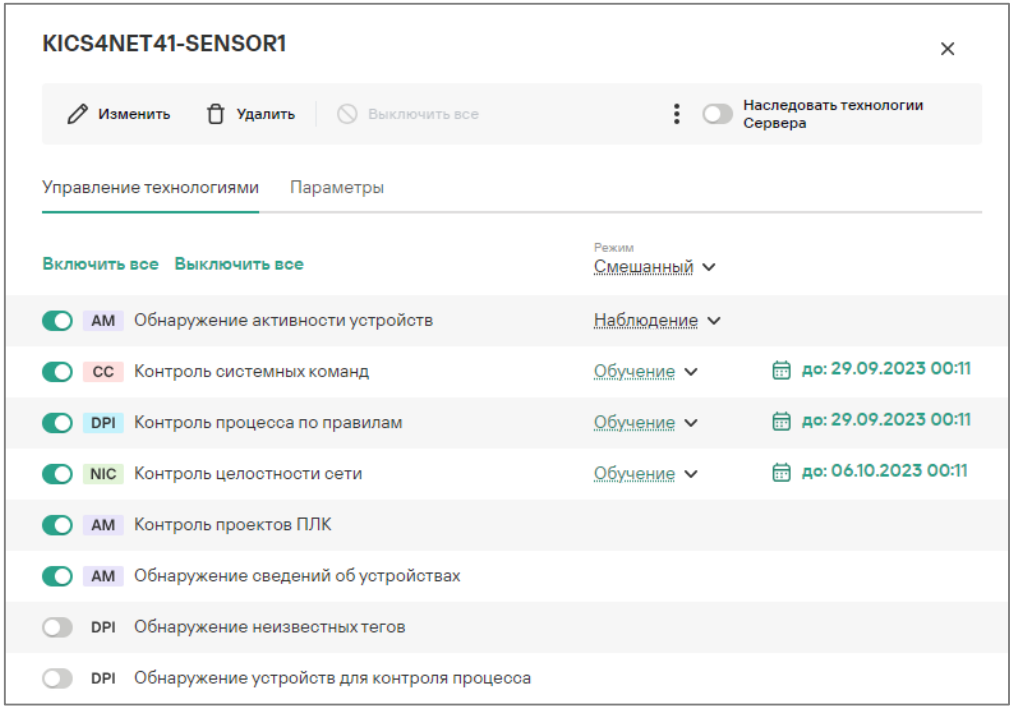


Оптимизация пространства, больше информации в карточке

Данные в карточке разбиты по секциям

Множество инструментов для работы с событиями и устройствами

Гибкие настройки обучения



Сенсоры и точки мониторинга могут наследовать настройки сервера или иметь свои

Удобно подключать новые площадки – пока вся система в режиме мониторинга, новая площадка может обучаться

Таймер на обучение – автоматическое переключение в режим мониторинга

Обновления продукта KICS for Nodes

Улучшения Firewall Management

- Гибкое управление уровнем интеграции
- Сканирование исходящего трафика
- Фильтрация по диапазону портов
- Разрешающие и запрещающие правила

Поддержка новых моделей ПЛК в модуле PLC Integrity Control: Siemens S7-1500, Prosoft Regul, ARIS, EKRA

Сертификация модуля контроля устройств (DC) и сертификация по МЭК 62443-4-1

Интеграция KICS и SD-WAN

2023

Мониторинг географически распределенных инфраструктур – множество необслуживаемых или обслуживаемых небольших площадок.

Решение: интеграция KICS и SD-WAN

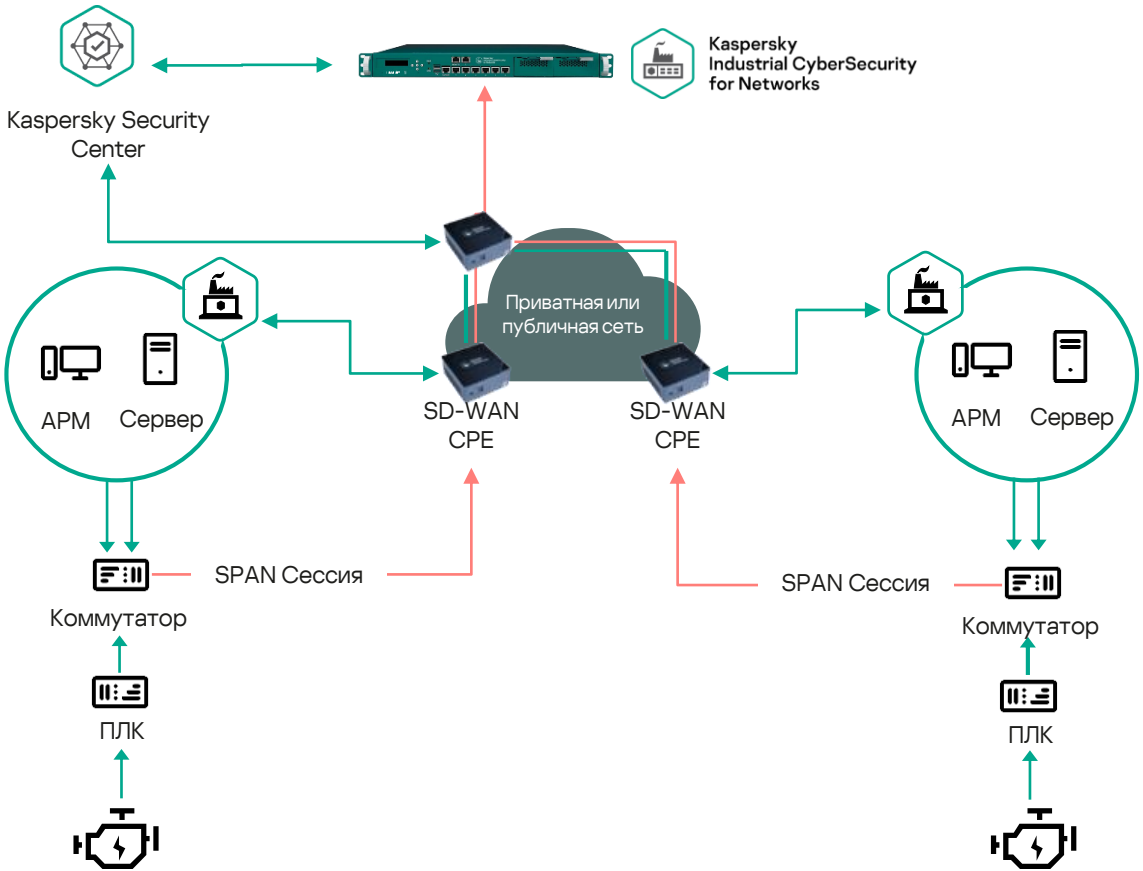
Возможность передачи SPAN-сессии напрямую с удаленного объекта на сервер/сенсор в HQ.

Масштабируемая транспортная сеть, через разные технологии доступа с дублированием каналов

Гибкая и легкая в настройке SD-WAN, есть компактное CPE

«Встроенный» мониторинг промышленного трафика!

Интеграция KICS for Networks и Kaspersky SD-WAN

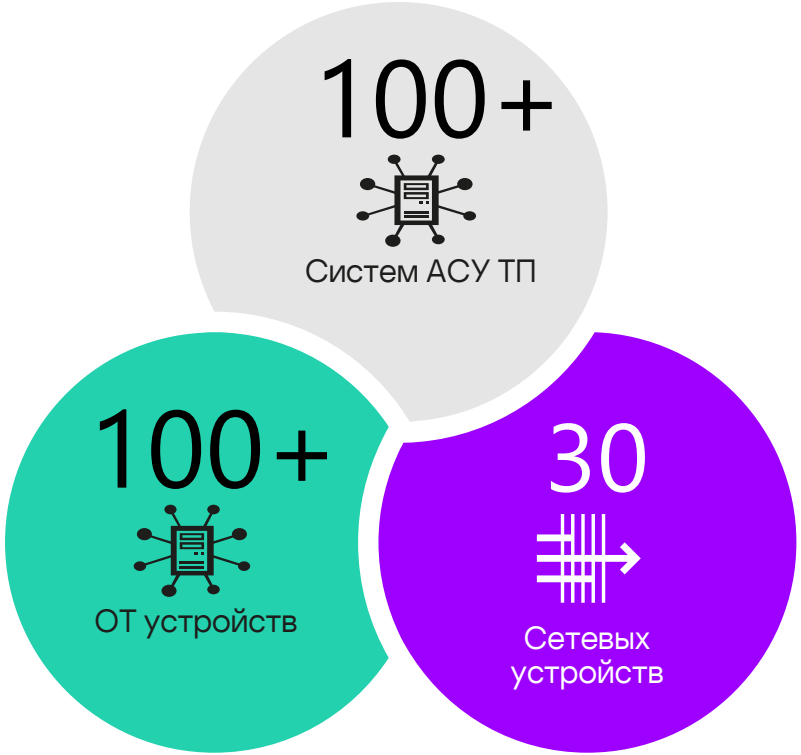


- Гибкость в создании распределённой инфраструктуры ИБ
- Компактное портативное устройство CPE, не требует много места
- SPAN-трафик передается на сервер или сенсор KICS for Networks в центральном офисе
- Разделение каналов внутри канала SD-WAN / поддержка различных сценариев, не влияющих друг на друга
- Поддержка резервирования через несколько каналов связи

Обновления ICS TI

2023

Обновления базы уязвимостей в KICS



- Пассивный анализ уязвимостей теперь поддерживает не только ПЛК, но и сетевые устройства

  Уже около 30 моделей поддержано

- Встроенные в KICS OVAL базы для детекта уязвимостей для более 100 различных АСУ ТП от более 20 вендоров (треть отечественных)

- Пассивный контроль целостности проекта ПЛК

- Импорт из SCADA проектов для устройств и тегов

Спасибо!

Ждем вас на демо!

Стрелков Андрей

Руководитель направления развития продуктов для промышленной безопасности

Telegram: @dogsraspberries

kaspersky